Computer & Communications Industry Association

1972-2012: 40 YEARS OF TECH ADVOCACY

Senate Commerce Committee
The Need for Privacy Protections: Is Industry Self-Regulation Adequate
June 28, 2012
Computer & Communications Industry Association Statement for the Record

Self-regulation is a vital part of consumer privacy protection, and the World Wide Web Consortium's current work on a Do Not Track standard, along with the Digital Advertising Alliance's agreement to honor a DNT header, are good examples of the power of this method. The Computer and Communications Industry is a 40 year-old international non-profit trade association dedicated to open markets, open systems, and open networks. CCIA members participate in many sectors of the computer, information technology, and telecommunications industries and range in size from small entrepreneurial firms to some of the largest in the industry. CCIA members employ nearly half a million workers and generate approximately a quarter of a trillion dollars in annual revenue.[1] Our members produce web browsers, operate search engines and e-commerce websites, are Internet advertisers, and offer free web services of many kinds.

Consumer choice regarding the use of personal data is of the utmost importance. Users should have the ability to opt-out of systems that impact their privacy if they're uncomfortable. This is important not just for reasons of pure privacy protection, but also because trust is so essential to the online marketplace. Users who don't trust an online service have many other competitors to choose from and can always take their business to another, more privacy-protecting, website.

[1] For a full CCIA member list, please see http://www.ccianet.org/index.asp?bid=11

Do Not Track options are an important part of consumer choice. These options allow users to indicate their preferences with regard to online tracking through a simple browser mechanism that is easy to set, universal, and permanent. A broad coalition of advertisers, brought together by government acting as a convener has agreed to honor the Do Not Track header. The World Wide Web Consortium (W3C), a multi-stakeholder body responsible for Web-wide technical protocols, is in the process of developing the specifications that will underpin the DNT header. This past week the W3C conducted a number of days of meetings surrounding the DNT header, and made progress on some of the remaining issues. A few outstanding questions remain to be answered before the specification is finalized.

As such, the W3C process is an example of a successful self-regulatory program. There are many different voices in the room there, each with strong opinions, but progress is being made and while the outcome is not yet certain, there is some confidence that an eventual agreement may be reached. There may be parties on all sides who are not entirely happy with the final result, but on the whole it will be a product of compromise and be a great step forward for privacy on the Internet.

In a parallel self-regulatory effort, a group of advertisers has come together called the Digital Advertising Alliance (DAA). The DAA has worked with government conveners to reach an agreement, backed by Section 5 of the FTC Act, to respect the DNT header. Self-regulation is alive and well in the tracking space, with companies, government, and civil society all collaborating to develop workable frameworks that protect users.

CCIA has two areas in which we wish to highlight concerns about the Do Not Track conversation. While the ongoing W3C process is a positive one, there are still a few areas where uncertainty remains, and where a wrong decision could have unintended consequences. By mentioning these areas, we hope to help avoid those consequences.

First is the question of exceptions to Do Not Track. The setting of a Do Not Track header, while it is an important consumer protection tool, cannot be a universal sign that a user will never have some traces kept surrounding their use of websites. There are important business reasons to monitor customer use of websites that should not be preempted by a Do Not Track header. For example, a lot of users' actions on websites are stored in order to combat fraud or cheating. Financial websites as well as essentially any online merchant must keep track of a certain amount of information about visitors in order to protect the entirety of their users.

For another example, the vast majority of websites anonymously track how users move around their own website in order to study their layout and usage statistics. We all reap the benefits of this tracking in the form of better website design and navigation, and website operators can improve their businesses by making sure visitors are finding the pages they need easily and quickly. This can be analogized to a retail store studying how anonymous visitors move through the store in order to decide if any changes need to be made to the layout of the products.

The second important aspect of Do Not Track is in user education. Do Not Track's focus is on the privacy implications of what can be collected on the web while a user browses. That information is of course very important to a user and should be a subject of education without a doubt. The problem here stems from what is not being adequately explained to users, and that is the value that comes from anonymized data. Advertising targeted toward what a person likes and enjoys pays for a huge amount of content and services on the World Wide Web that are offered for free to users. Without that source of revenue, innovation in online services would be much harder to come by as the price of starting up a new service and gaining customers willing to pay would be drastically higher.

Data isn't just important for advertising purposes. Collecting large amounts of anonymized data can open up worlds of research that users are not aware of. A famous example is Google's Flu Trends, in which computers analyze live queries coming from distinct geographical areas, highlighting people who are searching the Internet for flu symptoms. In this manner, Google can often predict flu outbreaks before even the Centers for Disease Control. Amazon and Netflix each do similar analysis when they help each of us find new books, movies, and music we might like, based on what thousands of other people have also enjoyed. This sort of data collection and analysis poses no real privacy threat, yet provides an invaluable public service.

Users today, however, are not presented with this side of data collection and are making decisions about privacy protection without understand this inherent tradeoff. If a user is fully educated and then makes a decision to remove herself from data ecosystem, that is a choice that should be respected, but the education must come first so that decision is informed.